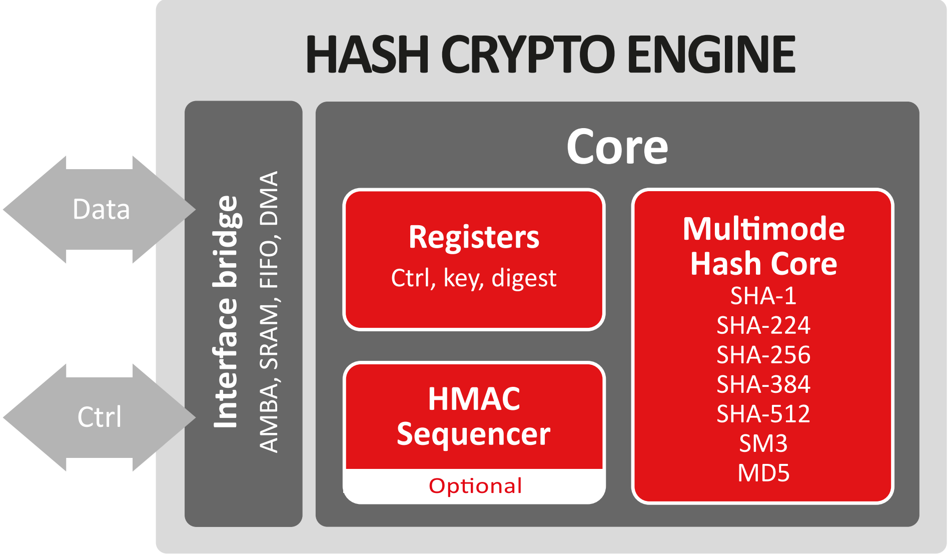
SILEX INSIGHT

Product sheet
BA413

HASH CRYPTO ENGINE

The Hash Crypto Engine is flexible and optimized hash IP core compliant with FIPS 180-3 (HASH functions), FIPS 198 (HMAC function) and OSCCA (SM3).

With a flexible wrapper supporting a wide selection of programmable hashing modes (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SM3 and MD5) with HMAC and several options of data interface, the Hash Crypto Engine is an easy-to-use solution with predictable resources and performances on ASIC and FPGA.



Features

- ✓ ASIC and FPGA
- ✓ Supports:
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512
  - SM3
  - MD5
- ✓ Supports HMAC
- ✓ Message padding in software or hardware
- ✓ Low power feature
- ✓ Data interface: AMBA (AHB/AXI) with optional DMA
- ✓ Control interface: APB/AXI4-lite

Applications

- ✓ Digital signature
- ✓ Key derivation

Implementation aspects

The Hash Crypto Engine is easily portable to ASIC and FPGA. It supports a wide range of applications on various technologies. The unique architecture enables a high level of flexibility. The throughput and features required by a specific application can be taken into account in order to select the most optimal and compact configuration.

Deliverables

- ✓ Netlist or RTL
- ✓ Scripts for synthesis & STA
- ✓ Self-checking RTL test-bench on referenced vectors
- ✓ Documentation

V1.2